SECURITY ISSUES FOR TELECOMMUTING

Information and telecommunications technologies make telecommuting an option for many organizations and workers. Organizations promote telecommuting to allow their employees to work from home, while on travel, at a client site, or in a telecommuting center. While offering potential benefits, telecommuting introduces new risks to the organization. This bulletin highlights security issues related to telecommuting and proposes solutions that may help organizations manage the telecommuting environment more effectively.

Telecommuting is the use of telecommunications to create an "office" away from the established (physical) office. The telecommuting office can be in an employee's home, a hotel room or conference center, an employee's travel site, or a telecommuting center. The telecommuter's office may or may not have the full computer functionality of the established office. For example, an employee on travel may read email. On the other side of the spectrum, an employee's home may be equipped with Integrated Services Digital Network (ISDN) access to provide the employee full computer capability at high speeds.

The Risk of Telecommuting

One of the popular buzz words for management in the '90s, telecommuting is becoming accepted as the way to do business. However, opening up an organization's information systems to dial-in and other forms of access presents significant security risks.

One risk is that intruders will be able to access corporate systems without having to be on site. Hackers, electronic eavesdroppers at conference sites, or shoulder surfers watching employees enter IDs and passwords, present very real threats. In addition to intruders whose goal may be mischief, hacking is attractive to people trying to steal or misuse corporate information. Electronic access to records may be difficult to trace and thus more appealing than trying to bribe employees or gain physical access.

Another risk of telecommuting is that corporate information can be read, and potentially modified, while it is in transit. Telecommuting also presents organizations with more commonplace risks. These include the risk of losing corporate information and resources when they are outside the protective shell of the organization.

Security Issues for Protecting Internal Systems

In planning for secure telecommuting, management must first determine what type of access is needed. What systems and data do employees need? What is the sensitivity of these systems and data? Do they need system administrator privileges? Do they need to share files with other employees? Is the data confidential?

From a security perspective, the critical determinations are:

- What would happen if an intruder gained the same access as the employee?
- What would happen if an intruder were able to use the employee's account, but gain more access than authorized for that user?

If these circumstances would result in the loss of organizational resources, managers must take steps to ensure that the integrity of their information systems is not compromised by telecommuting employees of the organization.

Firewalls/Secure Gateways

A secure gateway, called a firewall, blocks or filters access between two networks, often between a private network and a larger, more public network such as the Internet or public switched network (i.e., the telephone system). For telecommuting, organizations must decide what to make available to telecommuting employees using public networks, what degree to ensure that only authorized users can get to the internal network, and how to ensure that the secure gateway works properly.

If possible, managers should put all the resources needed by telecommuting employees outside of a secure gateway. However, this is only feasible if employees do not need access to corporate databases. For example, employees may only need to send reports in or access public databases, such as product/sales information or government forms.

However, most telecommuting employees require more access. For traveling employees, this may be limited to access to email. There are many firewall implementations that use an email proxy to allow access to the files on a protected system without having to directly access that system. However, some telecommuting employees need access to internal resources. The employees may need to use a variety of resources such as local area network (LAN) applications, mainframe applications, running client software, or Transmission Control Protocol/Internet Protocol (TCP/IP) services.

A secure gateway, or series of gateways, can be used to divide internal resources based on access need of telecommuters. For example, computers with high-risk organizational data (such as proprietary business plans) may be separated by a gateway from systems with a lower level of risk. A series of gateways can be used to further restrict access to the highest-risk systems. For some situations, current firewall technology can be used to give virtual access by using proxies. In addition, current firewalls can use IP filtering to limit access to certain types of resources.

For many organizations, the primary security function of the secure gateway is to provide robust authentication of users. Secure gateways may also provide additional auditing and session monitoring. The gateway can perform an intrusion detection function. For example, the secure gateway could monitor a session for keystrokes which may indicate someone trying to exceed access (e.g., ^C, ^Z).

Robust Authentication

For most organizations, robust authentication should be required if access is given to internal systems. However, organizations should require robust authentication even for email if it is relied upon to discuss business decisions (i.e., if the organization would care if someone else read your email).

Robust authentication increases security in two significant ways. It can require the user to possess a token in addition to a password or personal identification number (PIN). Tokens when used with PINs provide significantly more security than passwords. For a hacker or other would-be impersonator to pretend to be someone else, the impersonator must have both a valid token and the corresponding PIN. This is much more difficult than obtaining a valid password and user ID combination (especially since most user IDs are common knowledge).

Robust authentication can also create one-time passwords. Electronic monitoring (eavesdropping or sniffing) or observing a user type in a password is not a threat with one-time passwords because each time a user is authenticated to the computer, a different "password" is used. (A hacker could learn the one-time password through electronic monitoring, but it would be of no value.)

Most commercial robust authentication systems use smart tokens. The user provides a PIN which unlocks the token and then uses the token to create a one-time password. However, it is possible to use software-only one-time password schemes. (Tokens which do not provide for one-time passwords, such as automated teller machine (ATM) cards, are less common for telecommuting because they require hardware at the remote site and, without physical security, are vulnerable to electronic monitoring.)

Telecommuting employees who directly access internal systems should be robustly authenticated and should be routed to specific computer systems. The combination of robust authentication and routing increases security significantly and reduces costs associated with robust authentication by limiting it to employees with the greatest access.

It is possible, however, for an intruder to steal a session which had been originally authenticated with conventional or robust authentication. For applications with very high security concerns, authentication should be performed continuously through the use of cryptography. Other methods of performing continuous authentication, such as applying a digital signature to every packet, are being developed but are not currently widely available in commercial products.

The following figure diagrams an example of an organization with multiple access points for telecommuting that segregates telecommuters into three risk-based areas. Access to Host 1 is granted based on simple password-based authentication. Host 1 contains read-only applications. There is no confidential data on Host 1. Access to Host 2 is granted based on robust authentication, but is outside the firewall. The rationale for creating Host 2 is to be able to support applications that the firewall cannot protect against (e.g., no proxy is available). Access to internal systems (Host 3, Host 4, and the LAN) requires robust authentication. The firewall uses proxies to mediate between the external network (including both Internet and dial-in connectivity) and the internal network.

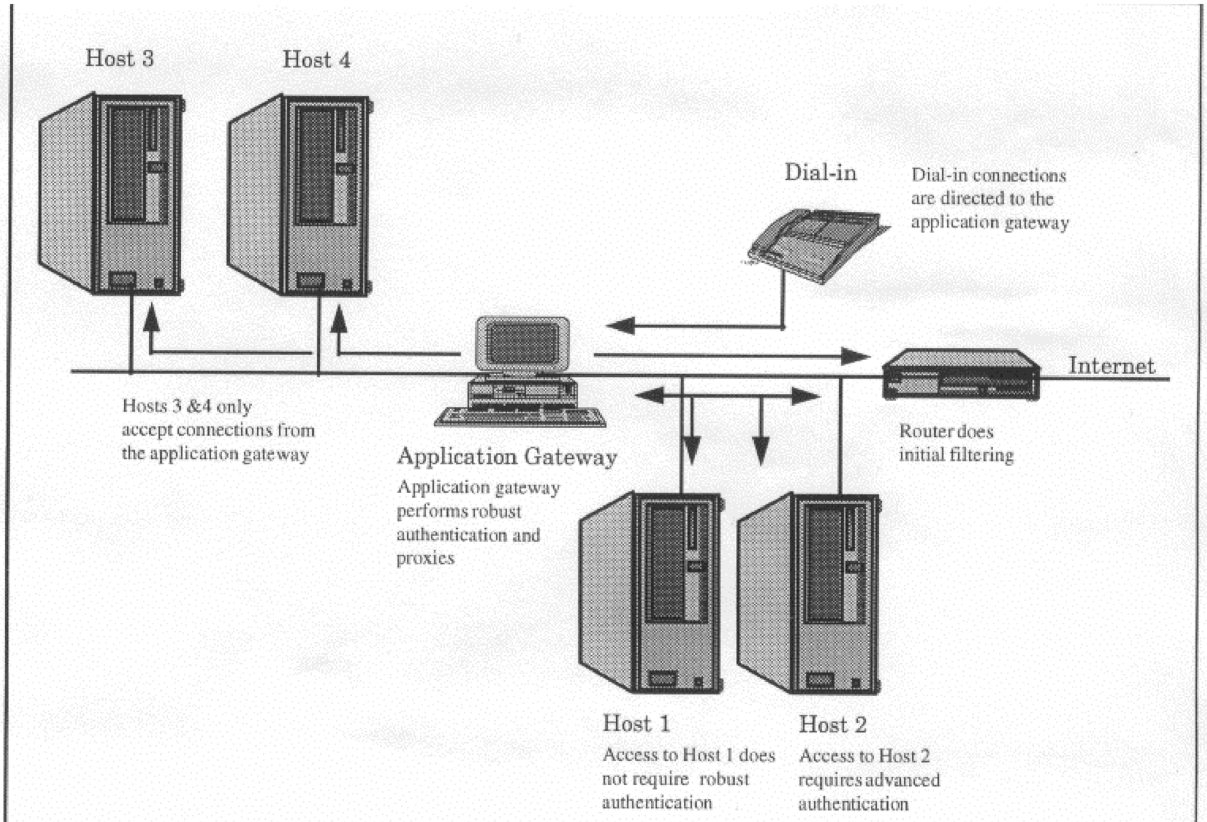
Host 3
Host 4
Dial-in
Dial-in connections are directed to the application gateway
Internet
Hosts 3 &4 only accept connections from the application gateway
Application Gateway
Application gateway performs robust authentication and proxies
Router does initial filtering
Host 1
Access to Host 1 does not require robust authentication
Host 2
Access to Host 2 requires advanced authentication

Figure 1, Protecting Internal Site Systems

Three caveats need to be made:

- Any additional logins (to Host 3 or Host 4, for example) are in the clear. Anyone eavesdropping on the connection can gain a valid ID and password to Host 3 or Host 4. With proper configuration management (i.e., no modem connections inside the firewall), these systems will not be directly accessible from the outside and the ID and password will not be usable.
- Too much or too complicated segregation may prevent users from sharing information necessary to perform their jobs.
- Firewall and router administration requires careful and correct implementation of rules (system-specific policy).

Port Protection Devices

A port protection device (PPD) is fitted to a communications port of a host computer and authorizes access to the port itself, prior to and independent of the computer's own access control functions. A PPD can be a separate device in the communications stream (typically PPDs are found only in serial communications streams) or it may be incorporated into a communications device (e.g., a modem). PPDs typically require a separate authenticator, such as a password, in order to access the communications port.

One of the most common PPDs is the dial-back modem. In a typical dial-back modem sequence, a user calls the dial-back modem and enters a password. The modem hangs up on the user and performs a table lookup for the password provided. If the password is found, the modem places a return call to the user (at a previously specified number) to initiate the session. The return call itself also helps to protect against the use of lost or compromised accounts. This is, however, not always the case. Malicious hackers can use such advanced functions as call forwarding to reroute calls.

Security Issues for Data Transfer

In addition to gaining access to internal systems, intruders can also eavesdrop on an entire session. Eavesdropping is not technically difficult if there is physical access to cable or wire used for communication or logical access to switching equipment.

If a telecommuting employee is transferring data that an eavesdropper would want, encryption may be necessary. Eavesdropping is more likely if an employee is at a large conference or other location where an eavesdropper may set up equipment in hopes of hearing something useful. Some conferences offer equipment to attendees to use to check email, transfer files, etc. Attendees find this useful, since they do not need to provide laptops; however, this could be a target for electronic eavesdropping.

Software- or hardware-based encryption provides strong protection against electronic eavesdropping. However, encryption is more expensive (in initial and operating costs) than robust authentication. It is most useful if highly confidential data needs to be transmitted or if moderately confidential data is transmitted in a high-threat area. Since employees do not always know when they are in a high-threat area, management must train employees to consider this potential threat.

Security Issues for Telecommuting from Home

In addition to risks to internal corporate systems and data in transit, telecommuting from home raises other concerns related to whether employees are using their own computers or using computers supplied to them by the organization.

Home Data Storage Integrity and Confidentiality

Other members of the employee's household may wish to use the computer used for telecommuting. Children, spouses, or other household members may inadvertently corrupt files, introduce viruses, or snoop. Organizations can take several approaches:

- Employee accountability. Some organizations may choose not to have specific rules forbidding household members from using personal computers (PCs), but hold the employee responsible for the integrity and confidentiality of the data. Obviously, if the data is highly confidential, this is not a good choice.

- Removable hard drives. If corporate data is stored on a removable hard drive (or floppy), the risk is greatly reduced.
- Data encryption. Corporate data can be kept encrypted on the hard disk. This protects its confidentiality and detects changes to files.
- Dedicated use. If an organization requires dedicated use, management should recognize that it is difficult to enforce.

Home System Availability

In addition to the possibility of failure or theft of a home computer, it may not be compatible with office configurations. For example, the home computer may use a different operating system. This and other circumstances may complicate set up, software support, troubleshooting, or repair. Organizations should ensure that policies are in place to cover all of these situations.

Security Issues for Telecommuting Centers

Telecommuting centers, normally located in outlying suburbs, offer another choice for organizations. From a security perspective, they may provide hardware for encryption, removable hard drives, and increased availability. However, by concentrating telecommuters, the centers may make themselves a more attractive target for eavesdropping. At a minimum, organizations should require robust authentication from telecommuting centers. If communications encryption is supported by the center, organizations should be aware that data may not be encrypted while it is inside the center. The encryption may occur at a modem pool.

Conclusion

In summary, telecommuting offers potential benefits to employees and organizations. With adequate attention to security, it is possible to create "an office away from the office."

References

Ascend Communications, **Telecommuting Network Planning Guide: A Resource Guide for Planners, Executives and Information Managers**, Alameda, CA.

Bill Boyle, *Cable & Wireless Staff are to Work from Home*, Computer Weekly, April 27, 1995, p. 6(1).

IDC Government, **Telecommuting: New Challenges in Information Security**, IDCG Pub. No.: W1831, March 1995.

NIST's Information Infrastructure Task Force Committee on Applications and Technology, **The Information Infrastructure: Reaching Society's Goals**, NIST Special Publication 868.

John Pescatore, *Telecommuting and Security Aspects*, Research Activity #9008, IDC Government, February 9, 1996.

Johna Till Johnson and K. Tolly, *The Safety Catch*, Data Communications Magazine, May 1995.

John P. Wack, and L. Carnahan, **Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls**, NIST Special Publication 800-10, December 1994.

http://www.telecommute.org/links.html#tc - includes resource links to new stories, organizations, teleworking studies, and telecommuting centers.

http://www.pacbell.com/Lib/TCGuide/tc-12.html - contains Pacific Bell's 4 page Telecommuting and Resource Access Security Checklist of questions to consider when creating a telecommuting security policy.